数理解析研究所講究録
第 1648 巻 2009 年 221-225

From Traditional Algorithmic Mathematics in Ancient China to Mathematics Mechanization in Modern China

Wu Wen-tsun[1]
MMKL, Academy of Mathematics and System Sciences, Academia Sinica
Beijing 100080, *P.R. China*

Abstract

In the first part of the present article we have described some characteristic features of traditional mathematics of ancient China quite different from those of ancient Greece which govern actually the development of present-day modern mathematics. Thus, in the Greek Euclidean system it is emphasized the theorems-proving based on logical reasonings on a system of axioms admitted in advance. On the other hand as already pointed out in the first part of the present article, our treatments lead naturally to polynomial equations-solving which becomes the central theme of developments of mathematics in ancient China. It has also been pointed out that such developments reach the climax in the time of Yuan Dynasty (1271-1368 A.D.). In fact, some scholar ZHU Szijse had outlined the general way of solving arbitrary systems of polynomial equations in arbitrary number of variables. In modern language it is equivalent to the determination of the whole set of zeros of a system of polynomial equations $P_i(x_1, x_2, \cdots, x_n) = 0, i = 1, 2, \cdots, N$, or the determination of the set of zeros $Zero(PS)$, with $PS = \{P_i \mid i = 1, 2, \cdots, N\}$. Of course in the period of ancient time the exhibition of ZHU cannot be so satisfactory in exactness and rigor from the point of view of modern mathematics. However, his line of thought and procedure are *precise* and *exact*. Based on these we shall describe below in modern language the procedure of ZHU, with some terminologies and techniques borrowed from the writings of J.F.Ritt (1893 - 1950 A.D.).

Let K be a field of characteristic 0, $X = \{x_1, x_2, \cdots, x_n\}$ a set of variables arranged in natural ascending order $x_1 \prec x_2 \prec \cdots \prec x_n$, and $R = K[X]$ be the ring of polynomials in X with coefficients in K. Any non-zero and non-constant polynomial $P \in R$ may now be written in the canonical form below:

---

[1] Second Part of an Article for Kyoto-Conference in Kyoto, Japan, March 8-9, 2006.

$$P = I_0 * x_c^d + I_1 * x_c^{d-1} + \cdots + I_d,$$

in which I_j are all either constants or polynomials in $x_1, \cdots, x_{c-1}$ alone with *initial* $I_0 \neq 0$. With respect to *class* c and *degree* d we may introduce a partial ordering $\prec$ for all non-zero polynomials in R with non-zero constant polynomials in the lowest ordering. Consider now some polynomial set either consisting of a single non-zero constant polynomoal or the polynomials may be so arranged with classes all positive and steadily increasing. Call such polynomial sets *ascending sets.* Then we may introduce a partial ordering $\prec$ among all such ascending sets with the trivial ones consistng of a single non-zero constant polynomial in the lowest ordering. For a finite polynomial set consisting of non-zero polynomials any ascending set wholly contained in it and of lowest ordering is called a *basic set* of the given polynomial set. A partial ordering among all finite polynomial sets may then be unambiguously introduced according to their basic sets.

With respect to a nontrivial asc-set $ASC = \{A_1, A_2, \cdots, A_r\}$ with steadily increasing positive classes any polynomial $P \in R$ may be written in a form

$$I_1^{h_1} * \cdots * I_r^{h_r} * P = \Sigma_{j=1,\cdots,r}\ Q_j * A_j + R,$$

in which I_i are initials of A_i, h_j are some non-negative integers which may be uniquely determined in lowest possible values, and R is a polynomial, if non-zero, of class less than that of A_1. The above formula is due to Ritt so it will be called *Ritt's Remainder Formula* and the actually uniquely determined polynomial R (eventually zero) will be called the *Remainder* of polynomial P with respect to the ascending set ASC.

For any finite polynomial set $PS \subset R$ consider now the scheme (S) below:

$$\begin{array}{lllllllll} PS = & PS^0 & PS^1 & \cdots & PS^i & \cdots & PS^m & & \\ & BS^0 & BS^1 & \cdots & BS^i & \cdots & BS^m & = & CS \\ & RS^0 & RS^1 & \cdots & RS^i & \cdots & RS^m & = & \emptyset. \end{array} \qquad \text{(S)}$$

In the scheme (S) each BS^i is a basic set of PS^i, each RS^i is the set of non-zero remainders, if any, of polynomials in $PS^i \setminus BS^i$ with respect to BS^i, and $PS^{i+1} = PS \cup BS^i \cup RS^i$ if RS^i is non-empty. It is easily proved that the sequences in the scheme should terminate at certain stage m with $RS^m = \emptyset$. The corresponding basic set $BS^m = CS$ is then called a *characteristic set* (abbr. *char-set*) of the given polynomial set PS. The *zero-set* of PS, $Zero(PS)$, which is the collection of common zeros of all polynomials in PS, is closely connected with that of CS by the *Well-Ordering Principle* in the form below:

$$Zero(PS) = Zero(CS/IP) \cup Zero(PS \ \cup \ \{IP\}),$$

in which IP is the product of all initials of polynomials in CS and $Zero(CS/IP) = Zero(CS) \setminus Zero(IP)$.

Now $PS \cup \{IP\}$ is easily seen to be a polynomial set of lower ordering than PS. If we apply the Well-Ordering Principle to $PS \cup \{IP\}$ and proceed further and further in the same way we should stopped in a finite number of steps and arrived at the following

Zero-Decomposition Theorem. For any finite polynomial set PS there is an algorithm which will give in a finite number of steps a finite set of asc-sets CS^s with initial-product IP^s such that

$$Zero(PS) = \bigcup_s Zero(CS^s \ / \ IP^s). \tag{Z}$$

Now CS^s are all ascending sets. Hence all zero-sets $Zero(CS^s)$ and all $Zero(CS^s / \ IP^s)$ may be considered as well-determined in some natural sense. The formula (Z) gives thus actually an explicit determination of $Zero(PS)$ for all finite polynomial sets PS which serves for the solving of arbitrary systems of polynomial equations.

As an application of above theory about polynomial equations-solving we would like to point out that it implies a method of proving usual geometry theorems. In fact, let T be a geometry theorem to be proved. In introducing some coordinate system in coordinates $\{x_i, i = 1, 2, \cdots\}$ the hypothesis will usually be expressed as a system of polynomial equations $HYP = 0$ in X and conclusion a polynomial equation $CONC = 0$ in X too. Let CS be the char-set of HYP. Let IP be the initial-product of CS, and R be the remainder of $CONC$ with respect to CS. Suppose $R = 0$. Then by Ritt's *Remainder Formula* and the *Well-Ordering Principle* we have

$$Zero(HYP/IP) \subset Zero(CONC).$$

This shows that $R = 0$ would imply that any geometric configuration verifying the hypothesis will verify the conclusion too, so far $IP \neq 0$. In other words, $R = 0$ is a sufficient condition for the theorem in question to be true under the subsidiary conditions $IP \neq 0$.

The above gives thus an effective way of proving geometry theorems, even discovering of new ones. Several hundred delicate geometry theorems have been thus proved and discovered for which we refer to the elegent book of CHOU Shang-Ching, *Mechanical Geometry Theorem-Proving*, Reidel, (1988).

The above method permits also to the discovery of *explicit* forms of unknown relations. As a simple example let us try to discover the explicit relation between the area and 3 sides of a triangle, necessarily exist but supposed unknown. For this purpose let us assign the values of the area and 3 sides to be x_0, x_1, x_2, x_3, while the coordinates of the vertices by x_i with $i > 3$. These values of $x_0, x_1, x_2, x_3, x_4, \cdots$

are necessarily connected by polynomial equations $P_j = 0, j = 1, 2, \cdots$. Let us form the charset CS of the polynomial set $\{P_j\}$. It is readily found that for the first one C_1 of CS, $C_1 = 0$ gives just the relation between x_0, x_1, x_2, x_3, viz. the well-known *Heron's Formula* which is now automatically discovered by means of computers. In the same way we may also automatically determine the expression of the volume of a tetrahedron in terms of its 6 sides, etc.

Our method of polynomial equations-solving had been extended to the differential case. The same is for the automatic proving and discovering of differential-geometry theorems, as well as the automatic determination of explicit relations between differential-geometric entities necessarily exist but unknown in forms. As a concrete example, it has been automatically discovered and determined the Newton's reciprocity square law of gravity attractive forces from Kepler's observational laws about planet motions.

As our method treats mathematics in an *algorithmic* or *mechanical* way by means of computers, so we have called it *Mechanization of Mathematics*, or **Mathematics Mechanization**.

As we have already pointed out, concrete problems, arising whether from mathematics, sciences, technologies, or else, will usually and naturally lead to solving of (eventually differential) polynomial equations, so our general method of solving arbitrary (eventually differential) polynomial equations will naturally lead to the solving of various kinds of problems arising from sciences and technologies, besides those from mathematics itself. This is really the case: We have applied our method to such problems arising from mathematics or non-mathematics partially listed below:

Engineering Mathematics,
Clifford Bracket Algebra for Geometry Computation,
Symbolic-Numeric Hybrid Computation,
Proving and Discovering of Inequalities, Geometric, Algebraic, Trigonometric, etc.
Optimization Problems, Global Optimization,
Non-linear Programming, Bilevel Programming, etc.,
Soliton-Type Solutions of Partial Differential Equations,
Yang-Mills Equations, Yang-Baxeter Equations, etc.,
Robotics, Inverse Kinematic Equations-Solving of Manipulators,
Stewart Platform and its Extensions by Enlarging Control Means,
Linkage Design, Machine Design,
PnP, particularly P3P,
Computer Vision,
CAGD, Surface-Fitting Problems, etc.,
Information Compression, Transmission, Safety Guarantee, etc.
Automatic Control,
Self-Satisfied Geometry-Expert Software and General Math-Mech-Software, etc.

For details we refer to various articles due to members of MMRC (Mathematics-Mechanization Research Center) of Institute of Systems Science, CAS, as well as their collaborators spread over the vast territory of modern China.